Net Arch Protocols

Daksh Dave
ddave@vt.edu

Final-Exam long Answer Problems

Q.1.a) IPv4 header : 20 bytes
TCP header : 20 bytes
TCP Payload : 1460 bytes
Total Length : 20+20+1460 = 1500 bytes

MTU = 900 bytes
DF = 0 MF = 0, fragmentation is allowed

Each fragment has its own header (20 bytes)

MTU - IPv4 header size => Maximum data payload per fragment
= 900 - 20 => 880 bytes

Data to fragment = 1500 - 20 => 1480 bytes

Data Must be in multiple of 8 bytes

First Fragment
Data Payload → 880 bytes

Remaining Data:
1480 - 880 = 600 bytes

Second Fragment:
Data Payload → 600 bytes

Total Fragments needed : 2

1.b) First frame (Maximum Size)

20 + 880 = 900 bytes

Second frame (Remaining Data)

20 + 600 = 620 bytes

c)

1.c) First Frame: length:
20 + 880 = 900 bytes
Offset = 0
MF = 1

Second Frame: length:
20 + 600 = 620 bytes
Offset = $\frac{880}{8}$ = 110

MF = 0

Frame	Total length	Offset	MF Flag
Frame 1	900	0	1
Frame 2	620	110	0

Q.3.a) Delay x Bandwidth

Bandwidth = 100,000,000 bits per second
RTT (Round-Trip Time) = 100 ms = 0.1 seconds

Delay x Bandwidth Product (bits)
=> Bandwidth x RTT = 100,000,000 x 0.1
=> 10,000,000 bits

Bits to Bytes
10,000,000 bits ÷ 8 = 1,250,000 bytes

= **1.25 MB**.

Standard TCP window size is 16-bit

0.3.b) Maximum TCP Window Size = $2^{16} - 1$

= 65,535 bytes

RTT = 0.1 s

Throughput (byte/s) = $\frac{\text{Window Size}}{RTT} = \frac{65,535}{0.1}$

= 655,350 bytes/s

Convert byte to bits per second

$655350 \wedge 8 =$ **5,242,800 bps**

Q.3.c) Smallest shift. cnt

Scaled Window Size ≥ Delay × B.W. Product

Standard Window Size = 65,535 bytes

Delay × Bandwidth = 1,250,000 bytes

shift. cnt = 1

Scaled window Size = 65535/2¹ = 131070 bytes

shift. cnt = 2

Scaled Window Size = 65535 × 2² = 262140 bytes

shift. cnt = 3

Scaled Window Size = 65535 × 2³ = 524280 bytes

shift. cnt = 4

Scaled Window Size = 65535 × 2⁴ = 1048560 bytes

* shift. cnt = 5

Scaled Window Size = 65535 × 2⁵ = 2097120 bytes

At shift. cnt = 5, scaled window size is 2097120 bytes which exceeds 1250000 bytes

2.a)

Step	Confirmed	Tentative
1	<R1, 0, –>	∅
2	<R1, 0, –>	<R2, 1, R2>, <R3, 6, R3>
3	<R1, 0, –>, <R2, 1, R2>	<R3, 6, R3>
4	<R1, 0, –>, <R2, 1, R2>	<R3, 5, R2>, <R4, 3, R2>
5	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>	<R3, 5, R2>
6	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>	<R3, 5, R2>, <R5, 4, R2>, <R6, 6, R2>
7	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>, <R5, 4, R2>	<R3, 5, R2>, <R6, 6, R2>
8	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>, <R5, 4, R2>	<R3, 5, R2>, <R6, 5, R2>
9	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>, <R5, 4, R2>, <R3, 5, R2>	<R6, 5, R2>
10	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>, <R5, 4, R2>, <R3, 5, R2>	<R5, 5, R2>
11	<R1, 0, –>, <R2, 1, R2>, <R4, 3, R2>, <R5, 4, R4>, <R3, 5, R2>, <R6, 5, R2>	∅

2.b)

Destination	Next Hop	Cost
R2	R2	1
R3	R2	5
R4	R2	3
R5	R2	4
R6	R2	5

4.a)

```
Airport ::= SEQUENCE {
Name IA5String,
IATACode IA5String,
NumTerminals INTEGER,
NumGates INTEGER,
City IA5String
}
```

4.b)

```
<?xml version="1.0" encoding="UTF-8"?>
< schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
  < element name="Airport">
    < complexType>
      < sequence>
        < element name="Name" type=" string"/>
```

```
      < element name="IATACode" type=" string"/>
      <element name="NumTerminals" type=" int"/>
      < element name="NumGates" type=" int"/>
      < element name="City" type=" string"/>
    </ sequence>
  </complexType>
 </ element>
</ schema>
```

5.a) Outer IP Header:

Source IPv4 Address: 203.0.113.222

Destination IPv4 Address: 233.252.0.14

5.b) Inner IP Header:

Source IPv4 Address: 198.51.100.11

Destination IPv4 Address: 198.51.100.77

5.c) **IPSec Mode: Tunnel Mode**

5.d)

IP Range: 198.51.100.224 to 198.51.100.255

Binary Representation:

198.51.100.224 → 11000110.00110011.01100100.11100000

198.51.100.255 → 11000110.00110011.01100100.11111111

The first 27 bits are identical: 11000110.00110011.01100100.111

Therefore, the subnet mask is /27.

This subnet covers 32 addresses (since 232−27=322^{32-27} = 32232−27=32), which aligns with the given IP range.

Final CIDR Notation: **198.51.100.224/27**